RECORD VERSION

STATEMENT BY

DR. LINTON WELLS II

PRINCIPAL DEPUTY ASSISTANT SECRETARY OF DEFENSE
(NETWORKS AND INFORMATION INTEGRATION)

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

ON

THE NEED TO KNOW: INFORMATION SHARING LESSONS FOR DISASTER RESPONSE

MARCH 30, 2006

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
HOUSE COMMITTEE ON GOVERNMENT REFORM

INTRODUCTION

Chairman Davis, Ranking Member Waxman, distinguished members of the Committee, thank you for inviting me here today to discuss the subject of information sharing lessons for disaster response. As the Principal Deputy Assistant Secretary of Defense for Networks and Information Integration (NII), I am representing Mr Grimes as the ASD(NII). This office recently designated a senior executive to serve as the Department's Information Sharing Executive.

I want to set the larger context for how information sharing and situational awareness are important not just to the Defense Department but to many processes the government is involved in. Warfare in the 21st Century, the core business process of the Defense Department, must be net-centric, meaning so well connected that well-trained professionals can self-synchronize their behavior with many others across vast distances, with devastating effect. Victory is dependent on discovering the enemy, accessing data, making decisions, and executing operations more rapidly and effectively than your adversary. Let me begin by saying that the communications and command and control (C2) lessons we are learning from the Federal, state, local, and commercial responses to Hurricane Katrina appear consistent with the lessons DoD has learned in the conduct of Humanitarian Assistance and Disaster Relief missions across the globe. Moreover, these lessons appear consistent with those lessons learned during stabilization and reconstruction operations in Afghanistan and Iraq. All of these situations involve high-levels of complexity, large populations, and the destruction of basic information and communications infrastructure. There is also a commonality of purpose that must be

organized, coordinated, deconflicted, and executed as efficiently and effectively as possible, using multiple sources of support – some of them totally unfamiliar with one another.

Communications – particularly wireless communications – are *the* critical enabler of all other functions in any disaster relief operation, along with the sensors to let you know what's happening and share the information and the ability to command and control those functions and information. These are all mission-critical functions. Hurricane Katrina was no exception. Without effective communications, every operation will suffer debilitating inefficiencies, some leading to ineffectiveness. My experience indicates that the first priority in both international and domestic situations is the establishment or restoration of wireless communications. Establishing or reestablishing communications has become a first-order requirement that must occur contemporaneously with rescue operations. Communication and information, when used appropriately, synergize the rescue response. It is imperative to take advantage of everyday technology to rapidly coordinate the rescue of our citizens across the entire spectrum of the crisis until its conclusion.

By now, the members of this Committee recognize that the Department of Defense and civilian responders from across the spectrum of Federal, state, and local authorities have matured into the post-September 11 world with different lexicons. The mission of fighting and winning this nation's wars is very different from responding to catastrophes spread across vast distances, regardless of their cause. Different lexicons are to be expected. America has a long tradition of carefully separating military and civilian

functions, especially in our homeland. My experience, however, tells me that when Mr. Canterbury of the Fraternal Order of Police testified before the House Government Reform Subcommittee on Emergency Preparedness, Science and Technology last year, his reference to command and control is the same concept that General Pace, Chairman of the Joint Chiefs of Staff, refers to using the same words. The ability to lead a complex organized operation requires situational awareness and the ability to communicate with everyone participating in that operation. The planning process establishes the social networks and procedures that give people the agility to adapt and overcome the unanticipated.

CATEGORIZING CHANGE

From my experiences since September 11, I have come to use a three-part construct to describe the actions necessary to ensure operability in catastrophic events internationally and domestically. These categories include: 1) technical capacity development; 2) "social network" development through planning, interaction, and collaboration; and 3) doctrinal changes and training.

TECHNICAL CAPACITY DEVELOPMENT

During the past 10 years, the U.S. military has honed its C2 skills in multiple deployments involving a mixture of war-fighting, civil affairs, humanitarian assistance, disaster relief and stabilization and reconstruction operations. The 1990s saw such deployments in Haiti and the Balkans, and they have only accelerated since the 9-11 attacks, with deployments in Afghanistan and Iraq. More recently, U.S. forces have been instrumental in providing key elements of the initial humanitarian responses to global

disasters, including the tsunami in Southeast Asia, the earthquake in Pakistan and Hurricane Katrina. All of these deployments have highlighted the increased need in the Department to communicate, collaborate, translate, and cooperate outside the closed networks required for military operations. Unlike the military, which always travels with its own power and infrastructure, civilian responders encountered command and control issues at the operational and tactical levels due to the devastation of the civilian-response infrastructure. Technology designed to operate without stable power sources in the austere environments of developing countries, is available today. Working with industry, these innovations can help to increase the survivability of tactical civil responder systems.

As stated earlier, when forces assigned to U.S. Northern Command and National Guard units deployed with military communications, they were once again ill-equipped to communicate with civilian responders struggling with a lack of communications infrastructure. Therefore, the Federal government must continue to expand its capability to rapidly deploy commercial-off-the-shelf networks making use of satellite links, wireless local area networks (LANs), laptop computers and "plug-and-play" equipment to bridge the gap created by a devastated civil infrastructure.

The lack of interoperability of first responders' communication equipment also hindered the effectiveness of operations. This problem won't be resolved by everyone buying the same product. It may be solved through collaborative efforts involving spectrum allocation and agreement both within industry and in the first responder

community on common data standards. In the near term, we must continue to encourage the development and purchase of technology that bridge these disparate systems.

SOCIAL NETWORK DEVELOPMENT

Much of the work that needs to be done at the strategic level in the wake of what we have learned revolves around social networks rather than any lack of technology. Hurricane Katrina showed us that a key source of the problem stemmed from a lack of familiarity with each other's operating practices – what DoD calls tactics, techniques, and procedures. What was lacking was familiarity with the National Response Plan, a shared understanding of how NORTHCOM was to support that plan, and experience gained through exercises between U.S. military and Federal, state, and local responders. A nationally focused effort to generate a truly collaborative information environment is feasible through coordinating the resolution of legal, policy and technical issues across all agencies and all levels of government. Ideally, there would be full interoperability among systems for command and control, communications, computers, intelligence, surveillance, and reconnaissance (known together as "C4ISR"). In addition, there needs to be broader, more fully articulated planning for multiple kinds of disaster events, ranging from natural disasters such as Hurricane Katrina up through a nuclear strike. Command and control, which is a social process augmented by communications and information, must extend to all appropriate locations, from a local sheriff's car to the White House. Moreover, we must exercise and train in a common environment to be better prepared to respond to such crises in the future.

Multiple efforts have addressed, or are addressing, segments of the need for a national response capability. These include:

- National Security Telecommunications and Information Systems - Developing plans and programs, including the development of architectures, to ensure security on National Security Systems;

- Continuity Communications Enterprise Architecture – Architecture to enable the Federal Executive Branch to execute mission-essential functions under all circumstances;

- Intelligence Community Architecture – Architecture to enable the intelligence community to share information;

We must vigorously support collaborative planning and interoperability at all levels of government, ensuring that decision-makers have unencumbered access to the best available information and enabling interoperable command and control operations. The Federal government must have command and control capabilities, supporting facilities, and infrastructure to ensure uninterrupted connectivity and coordination in support of essential functions in accordance with constitutional authorities. Our goal should be to provide assured services across government by:

- Making information available on a network that is dependable and trusted,

- Providing the available and appropriate bandwidth, frequency and computing capabilities within the spectrum management process,

- Assuring appropriate and effective collaboration capabilities and other performance support tools,

- Supporting secure and assured information sharing, without disadvantaging the responder lacking a security clearance,

- Continuously refreshing the information content of a shared situational awareness capability,

- Promoting infrastructure transparency (to the user),

- Assuring independence of information and data for consumers and producers,

- Considering that all users of information are also suppliers (and therefore encouraging parties to contribute data rather than just downloading it),

- Supporting information transactions that are asynchronous in time and place,

- Supporting the disadvantaged user with intermittent access to limited data services, and

- Applying federal data tagging standards and information assurance policies.

I have learned a great deal about "social networks" in the international context in the past three years. It is critical to develop purposely professional and personal links among experts and practitioners from multiple fields and sectors in humanitarian relief, disaster relief, and stabilization and reconstruction operations. These ties, built up over time and through enormous effort, are absolutely vital to organizing an effective response when catastrophic disasters occur. Unless working arrangements to communicate and share information among all of these types of entities can be formulated, the success of

any operation can be compromised, with results that can prolong or even exacerbate the effects of the disaster. Extensive planning and training is essential before the crisis.

DOCTRINAL CHANGES AND TRAINING

In the area of doctrinal change in the international context, DoD is embracing the concept of "integrated operations." This reflects a new battlespace management concept that will transform our military competencies from joint operations to operations that are fully integrated and coordinated with those of the military's partners in an operation. In the case of humanitarian assistance activities, these partners may include other U.S. agencies, allied militaries and governments, nongovernmental organizations, local populations, and private industry. And to maximize our effectiveness, DoD will integrate from planning to execution and then on to the transition to a restored local authority. Employing a coherent strategy that uses all instruments of the state in concert will ensure success in relief operations over the long term.

This doctrine also better prepares DoD to fulfill domestic response missions, bringing together civilian responders and military planners to synergize their efforts. Within the United States, DoD has conducted many scenario-driven exercises designed to prepare the military to support humanitarian assistance across a broad range of natural disasters – and also with regard to protecting potential terrorist target sites. Exercises and training opportunities between the U.S. military and civilian responders are critical to achieving this level of integration.

INFORMATION SHARING INITIATIVES

At this point, I would like to discuss some specific initiatives promoting the Information Sharing culture, a pilot effort with the Coast Guard, lessons learned with current techniques for regional information exchange, and a list of challenges we face as we prioritize and solve Inter-Agency infrastructure and information sharing efforts.

PROMOTING A CULTURE OF INFORMATION SHARING

The National Defense Strategy identifies "Conducting Network-Centric Operations" as one of the key operational capabilities required for defense transformation. The Department is transforming by building the foundation for net-centric operations in policy, program oversight, resource allocation, and cultural areas. Transforming to a net-centric force requires fundamental changes in all areas to provide the necessary speed, accuracy, and quality of decision-making critical to future success. Domestic response missions will benefit from this transformation and especially from two transformation initiatives promoting a culture of information sharing within DoD.

A cornerstone initiative is embodied in the DoD Net-Centric Data Strategy which outlines the vision for making data visible, available, and understandable--when needed and where needed--to accelerate decision cycles. The concepts in the Data Strategy are implemented through policies and actions carried out by Communities of Interest (COI) which are comprised of representatives from Combatant Commands, Services, Agencies and, where applicable, external partners. A COI is a community of people who are

interested in the same subject and need to share information to resolve mission issues that affect their community.

The second initiative is achieving assured information sharing via transformation in Information Assurance (IA). As users, services, information, and networks are co-resident within a net-centric information sharing space, data encryption boundary protection requirements must now shift to each object, device, and user within DoD's Global Information Grid (GIG). Robust IA must be applied throughout the GIG to protect it against cyber warfare attacks. An assured enterprise requires enterprise level governance, systems engineering, policy, risk management, operational doctrine, and training properly integrated with technology. Achieving agreement on these aspects of an enterprise across the diverse set of DoD components, Services and Agencies, the Intelligence Community (IC), Department of Homeland Security (DHS), other Federal Agencies, state and local governments, tribes, non-government organizations, and our foreign partners is a major challenge. The IA component of the GIG Integrated Architecture, developed under the purview of the National Security Agency (NSA), provides an IA strategy for achieving the assured, integrated, and survivable information enterprise necessary to attain the strategic objectives of the DoD and IC. Additionally, DoD is focusing on some very specific information sharing initiatives.

INFORMATION SHARING ENVIRONMENT – EXECUTIVE ORDER 13388

Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans" makes clear the President's intent to ensure that the heads of all Federal departments and agencies who "possess or acquire terrorism information shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions". Under the leadership of the Director of National Intelligence (DNI), DoD is fully engaged in supporting specific products such as establishing common standards for how information is acquired, accessed and used, addressing policy issues that inhibit information sharing and developing a common framework for information sharing between executive departments law enforcement agencies and state, local and tribal governments. An implementation plan is due in July of this year.

MARITIME DOMAIN AWARENESS (MDA) DATA SHARING PILOT

The Department of Defense (DoD), represented by US NORTHERN Command, in partnership with the Department of Homeland Security (DHS), represented by the United States Coast Guard, established a Maritime Domain Awareness Data Sharing Community of Interest (MDA DS COI) in February 2006. The MDA DS COI is piloting web-based data services to improve maritime situation awareness supporting Federal, State, Local, Tribal, Commercial, and international partners tracking vessels, cargo, and people of interest. This community-based pilot will develop a common vocabulary, and data services rendering maritime data visible, accessible, and understandable for authorized data users. The data users will post their data with

appropriate context-related tags to improve the precision of subsequent data discovery and understanding. This effort is identifying and documenting a repeatable process to be applied to additional data sources in future pilot spirals for MDA and will be examined for applicability to other information sharing challenges. The MDA DS COI pilot goal is to demonstrate a methodology to increase maritime situational awareness and improve the security and defense of US borders and interests though the detection, tracking, interception, or interdiction of vessels, cargo, and people of interest within the maritime domain.

INFORMATION SHARING WITH OUR COALITION PARTNERS

In the execution of warfighting and stability operations, the ability to support combined operations is enhanced by sharing information among the participants. Currently, the primary network used by US Combatant Commanders to plan and execute operations is the Secret Internet Protocol Router Network or SIPRNET. Sharing information with coalition members in Afghanistan and Iraq requires three different networks. Information deemed releasable on the SIPRNET is downloaded onto separate media and transferred to be uploaded into the other networks.

The U.S. in collaboration with the United Kingdom, its key coalition partner, has established a senior body to bring greater information sharing capability to the warfighter quickly and be ready to fight together on the first day of the conflict. Mr. Grimes sits on this group, the U.S.-U.K. Interoperability Commission, along with Mr. Ken Krieg, the Under Secretary of Defense for Acquisition Technology and Logistics, and Lt Gen Fulton of the U.K. Our objective is to bring enhanced information sharing capability to the field today while ensuring a seamless transition to the future net-centric environment

envisioned by the U.S. and U.K. The U.S. is supporting the U.K.'s upcoming deployment into Afghanistan with real capability to share a common understanding of the battle space. My team, working with the U.K., is implementing the capability to share the Afghanistan common operational picture directly from the SIPRNET to the U.K. Joint Operations Center system so it can provide the U.K. Commander with a robust understanding of his operations area. This capability is expected to connect national command and control systems directly, removing the burden of transferring information from national systems to the appropriate network for sharing. These initial steps in a bi-lateral environment are laying the groundwork for greater information sharing when coalitions are involved. We are moving to provide greater combat effectiveness for U.S. forces and the entire coalition.

INTER-AGENCY INFRASTRUCTURE WORKING GROUP

The DoD CIO office has established a working group with representatives from many of the Federal Departments (DHS, State, DOJ) to identify and resolve issues that inhibit the seamless exchange of relevant information. Some of the issues the working group is addressing include: (1) governance (2) resourcing and prioritization of initiatives (3) synchronizing of efforts (4) reconciling interdepartmental missions, strategies, and objectives, and (5) trusted security accreditation.

In closing, allow me to reiterate that the road to effective information sharing and situational awareness for the Department of Defense will be realized through our net centric approach to data sharing and information assurance, our continued supremacy in

state of the art communications equipment, our pursuit of the values that embrace a "sharing" culture and a commitment to changing our own doctrine and training structures. This endeavor, however, is a journey…not a destination.

Thank you for the opportunity to address the Committee.